February 9, 2001

INSPECTOR GENERAL INSTRUCTION 7950.2

SUBJECT: Microcomputer Hardware and Software Management Program

References: See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), Microcomputer Hardware and Software Management Program.

B. Cancellation. This Instruction supersedes IGDINST 7950.2, *Microcomputer Hardware and Software Management Program*, May 23, 2000.

C. Applicability and Scope. This Instruction applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; and the Director, Intelligence Review. When appropriate, the Office of the Deputy General Counsel (Inspector General) shall coordinate microcomputer hardware or software issues. For purposes of this Instruction, these organizations are referred to collectively as OIG components. The standards apply only to microcomputer hardware and software and only to that hardware and software for which there is a wide requirement within the OIG.

D. Definitions. See Appendix B.

E. Policy

1. The OIG, DoD, shall emphasize standardization and compatibility of microcomputer hardware and software.

2. The Information Systems Directorate (ISD), Office of Administration and Information Management (OA&IM), shall support and manage OIG, DoD, standard microcomputer hardware and software.

3. The use of nonstandard hardware or software is a component-level management decision. The ISD shall not support microcomputer hardware or software that the Chief Information Officer (CIO) has not declared an OIG standard. Any OIG component or end user that chooses to use nonstandard microcomputer hardware or software is responsible for the functioning of those information resources. That includes any effect that microcomputer hardware or software may have on the operation of standard microcomputer hardware and software. Even virus-free information resources may cause conflicts when introduced into the OIG, DoD, environment. If the ISD determines that introduced microcomputer hardware or software are causing malfunction of standard microcomputer hardware or software, the ISD will return the user to the standard configuration. The ISD will not assume responsibility for any functionality or data lost by return to the standard configuration. Any exceptions to this provision must be negotiated between the component and the ISD.

4. All previous software standards supported by the ISD as of the publication date of this Instruction will continue to be supported until the CIO declares the changeover to revised OIG, DoD, standards is complete.

5. In accordance with reference a, the ISD, the Personnel and Security Directorate (PSD), OA&IM, and the OIG components shall prepare plans for ensuring that microcomputer hardware and software used in sensitive information systems have appropriate safeguards and controls to prevent loss or harm to the information and to maintain system security, integrity and availability. The OIG components shall implement and maintain such plans after approval by the Designated Approving Authority (DAA), as defined in Appendix B. Approval to operate must be in compliance with reference e. Microcomputer hardware and software intended for processing Sensitive Compartmentalized Information (SCI) must be security certified and accredited by the DAA.

6. The microcomputer hardware shall be Microsoft compatible and shall meet minimum specifications defined by the ISD.

7. The OIG, DoD, microcomputer software standards are as follows:

a. *Microsoft* compatible operating environment software.

b. *Microsoft Access* as the relational data base management package.

c. *Microsoft Word* as the word processing package.

d. *Microsoft Excel* as the spreadsheet package.

e. *Microsoft Power Point* as the presentation graphics package.

f. *Norton Corporate Edition* as the virus checking package.

g. *Microsoft Outlook* as the E-Mail and calendar program.

h. Additional standards (available as justified) are:

(1) *ProComm Plus* as the telecommunications package.

(2) *Netscape Navigator* as the browser package.

(3) *Microsoft Internet Explorer* as the special needs browser package.

(4) C2 compliant software required to process classified information.

8. The Information System Liaison Working Group shall propose additional or changes to OIG, DoD, standards, according to the procedures outlined in reference a.

9. Information systems security should be incorporated into all unclassified or classified automated information systems (AIS). Before selecting hardware or software, the following safeguards will be considered: physical security, personnel security, need-to-know, administrative security, information systems security, and emissions security.

F. <u>Responsibilities</u>

1. The **CIO** shall approve OIG, DoD, microcomputer hardware and software standards.

2. The **ISD** shall, as soon as the CIO approves a standard:

a. Manage OIG, DoD, standard microcomputer hardware and software in accordance with references b through i, and other applicable laws, guidelines, regulations, and standards, internal and external. That includes, but is not limited to, public laws and OIG, DoD, General Services Administration (GSA), DoD, and Office of Management and Budget (OMB) publications.

b. Review the requirements documentation submitted by the components, in accordance with reference f.

c. In coordination with the OIG components, perform the full range of configuration management. That includes determining what versions, implementation environment, and models of the OIG, DoD, standards will meet stated functional and technical requirements.

d. Provide end user support regarding OIG, DoD, standard microcomputer hardware and software.

e. Analyze proposed additional or changed OIG, DoD, microcomputer hardware and software standards, including costs and support plans.

f. Maintain trend analysis data on hardware and software performance as a means to identify root causes of recurring problem areas.

g. Serve as the OIG, DoD, Network Security Manager (NSM) responsible for the functional security operation of the network. The NSM ensures that the network complies with the requirements for interconnecting to external systems.

h. Provide contracting acquisition support for approved nonstandard hardware and software when the price exceeds the acquisition limit of the component's International Merchant Purchase Authorization Card (IMPAC).

i. Ensure all OIG, DoD, microcomputer hardware and software complies with applicable security laws, guidelines, and standards.

3. The **PSD, OA&IM,** shall:

a. Develop AIS security policies, standards, and procedures, to include the use of hardware and software.

b. Perform duties delegated by the DAA regarding any OIG, DoD, microcomputer hardware or software that process sensitive materials in accordance with reference b.

c. Advise and assist management on appropriate administrative action(s) if misuse occurs.

4. The **Component Heads** shall:

a. Develop functional requirements documentation for microcomputer hardware and software in accordance with reference f.

b. Develop procedures for component-level management of microcomputer hardware and software in their mission areas, including monitoring use to ensure that:

(1) All microcomputer hardware and software are used, safeguarded, accounted for, and disposed of in accordance with established policy, laws, licensing agreements, and guidelines, and

(2) There is adequate capability to support and maintain any nonstandard microcomputer hardware and software within the OIG component, or

(3) If requesting ISD support and maintenance for nonstandard microcomputer hardware or software, extraordinary circumstances exist that justify a written, negotiated agreement.

c. Communicate their decisions regarding use of nonstandard hardware or software to their users.

5. The **Information Systems Liaison Working Group**, as defined in reference a, is responsible for monitoring microcomputer hardware and software requirements, and proposing additional or changed OIG, DoD, standards.

G. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

/signed/
Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

APPENDIX A
REFERENCES

a. IGDINST 8000.1, Inspector General Automated Information Systems (AIS) Management, February 1, 2001

b. IGINST 5200.40, Security Requirements for Automated Information Systems, July 20, 2000

c. DoD Directive 7950.1, "Automated Data Processing Resources Management," September 29, 1980

d. DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992

e. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AIS)," March 21, 1988

f. IGDINST 7950.1, Acquisition of Information Technology Resources, May 23, 2000

g. IGDINST 7920.5, *Inspector General Small Computer Use*, August 18, 2000

h. IGDM 7200.10, Accountable Property Management Program, September 30, 1994

i. Computer Security Act of 1987, Public Law 100-235

APPENDIX B
DEFINITIONS

a. **Accountable Property Officer** is an individual appointed, in writing, by the proper authority, who maintains item and/or financial records in connection with OIG, DoD, accountable property, irrespective of whether the property is in his/her possession for use or storage, or is in the possession of others to whom it has been officially entrusted for use, care, or safekeeping.

b. **Accreditation** is a DAA's assertion of an acceptable level of security risk of an Information System (IS) and its environment. Acceptable security risk is the expectation that an IS will provide adequate protection against unauthorized access, alteration, or use of resources, and against denial of service to authorized users of the IS.

c. **Certification** is the comprehensive evaluation of the technical and non-technical security features of an IS and other safeguards, made as part of in support of the accreditation process, to establish the extent to which a particular design and implementation meet a specified set of security requirements.

d. **Chief Information Officer (CIO)** is the senior official, appointed by the Inspector General, DoD, to be responsible for developing and implementing information resources management in ways that enhance OIG, DoD, mission performance through the effective, economic acquisition, and use of information. The current CIO is the Director, Office of Administration and Information Management.

e. **Configuration Management** is accounting for, controlling and reporting the planned and actual design of an automated information system throughout its operational life. This includes the microcomputer hardware and software configuration, including the versions, models, and environments to be implemented.

f. **Designated Approving Authority (DAA)** is the official, appointed by the Inspector General, DoD, who has the authority to accept the security safeguards prescribed for an information system. The DAA issues an accreditation statement that records the decision to accept those standards. The current DAA is the Director, Office of Administration and Information Management.

g. **End User** is an OIG, DoD, employee or contractor who uses automated equipment to perform work-related tasks.

h. **End User Support** includes diagnosing and resolving problems about operating and using standard OIG, DoD, microcomputer hardware, software, telecommunications, and software applications.

i. **Environment** includes elements and mode of operation of an automated information system.

j. **Functional Requirement** is an expressed microcomputer hardware or software capability needed to accomplish the OIG, DoD, mission in a more efficient, effective, or economical manner. A functional requirement may fulfill a need for a capability previously unidentified, correct a shortcoming or deficiency in current OIG, DoD, standards or improve mission effectiveness or efficiency.

k. **Hardware** is the equipment supporting an automated information system.

l. **Information** is any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, maintained in any medium, including but not limited to, computerized data bases, paper, microform, or magnetic tape.

m. **Information Resources** are any combination of microcomputer hardware, software, and telecommunications, along with documentation and automated and manual procedures, that provide the information necessary to accomplish organizational missions and objectives.

n**.** **Information System** is the organized collection, processing, transmission, and dissemination of information according to defined procedures, whether automated or manual. It includes people, equipment, and policies.

o. **Microcomputers** are computers that have self-contained processing units and are easily transportable. The definition includes, but is not limited to, equipment that may be referred to as personal computers, desktop computers, laptops, palmtops, and notebooks.

p. **Network Security Manager (NSM)** is the individual responsible for the overall security operation of the network and is the focal point for policy, guidance, and assistance in network security matters. In addition, the NSM ensures that the network complies with the requirements for interconnecting to external systems.

q. **Property Custodian** is an individual appointed in writing by the proper authority to exercise proper custody, care, and safekeeping of OIG, DoD, accountable property entrusted to his or her possession or under his or her supervision. He or she may incur pecuniary liability for losses because of failure to exercise his or her obligation.

r. **Sensitive Unclassified Information** is any information that if lost, misused, disclosed, or destroyed, could adversely affect the national interest or the conduct of OIG, DoD, operations or Federal programs, or the privacy to which individuals are entitled under the Privacy Act. Typical types of data that are considered sensitive are "For Official Use Only," proprietary, financial, and mission critical information.

s. **Software** is a pre-written program used to perform a specific task, such as word processing, desktop publishing, etc.

t. **System** is a collection of people, equipment, policies, and methods organized to accomplish an activity.